REMARKS

This paper is responsive to an Office Action mailed on March 8, 2007. Prior to this response, claims 1-2, 4-14, and 16-27 were pending. Claims 1-2, 4-14, and 16-27 remain pending.

In Section 4 of the Office Action claims 1-2, 4-9, 11-14, 16-23, and 25-27 have been rejected as unpatentable under 35 U.S.C. 103(a) with respect to Seder et al. ("Seder"; US 6,694,043) in view of Dutta (US 2002/0138759). With respect to claims 1, 13, 14, and 26-27 the Office Action acknowledges that Seder fails to disclose profiles having an address field and an encryption field, the encryption of a document in response to the encryption field of a selected profile, or the sending of a profile in response to the address field of a selected profile. The Office Action states that Dutta discloses the use of encryption to shield an address, and the use of key to decrypt the address. The Office Action further states that it would have been obvious to combine the teachings of Seder with Dutta because "the use of encryption shields a recipient's/sender's address [0015] which is in response to the address of the selected profile in order to decrypt the encrypted data to yield recipient's address [0030]." This rejection is traversed as follows.

An invention is unpatentable if the differences between it and the prior art would have been obvious at the time of the invention. As stated in MPEP § 2143, there are three requirements to establish a *prima facie* case of obviousness.

> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the

> art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck* 947 F.2d 488, 20 USPQ2d, 1438 (Fed. Cir. 1991).

Generally, Seder describes a stenanographic encoding system which creates a watermark that is (invisibly) superimposed on a document. Upon photographing the document, the watermark can be detected. Once identified, the watermark may be used to prompt an action, such as identifying the file name of the document (col. 1, ln. 30-54).

Dutta discloses a parcel or physical document delivery system that uses encryption to shield the recipient's or sender's address that is printed on the physical medium. The invention generates encryption keys and provides encrypted data for display on an envelop [0004]. Dutta's encryption keys may be either symmetric or public keys [0015]. A scanner may be used to read an encrypted address printed on a physical envelop [0016] using keys retrieved from a secure database [0017-0018]. As shown in Fig. 1, upon submission of their name and address, a recipient receives a key. When a parcel is sent, encrypted data is printed on the package instead of a plaintext address. To guide the package through routing and delivery, the delivery agency decrypts the encrypted data printed on the parcel [0030, 0036, and 0042]. In summary, Dutta discloses a delivery agency that supplies a sender with a key for encrypting data to be used in place of a plaintext address printed on a parcel. The delivery agency decrypts the address upon receipt from the sender, so that the parcel can be delivered to its intended destination. The Applicant notes that Dutta is absolutely silent on the subject of a

computer text file (profile) that includes an address field and an encryption field. While Dutta's system does permit a user to request an encryption key to be used in the generation of encrypted addresses, Dutta's system not permit a user to select a profile (as defined above). In fact, since the delivery agency supplies the keys to the sender [0030] it appears as if the sender is unable to select the type of encryption that is used.

With respect to claims 1, 13, 14, and 26-27, the Seder and Dutta references have been combined based upon the assumption that the combination discloses all the claimed invention limitations. However as noted above, the Office Action acknowledges that Seder fails to disclose a profile with address and encryption fields, the use of such a profile encryption field to encrypt a document, or the use of a profile address field as the document destination. Likewise, Dutta fails to disclose a profile with address and encryption fields, or the selection of a profile. Further, Dutta fails to disclose the use of a selected profile encryption field to encrypt a document. Dutta's system does not permit a user to selection the encryption means. Further, Dutta's system does not encrypt the delivered document, only addresses are encrypted.

With respect to the third *prima facie* requirement, even if Seder and Dutta are combined, they do not explicitly disclose all the limitations of claims 1, 13, 14, 26, and 27. Claims 2, 4-9, and 11-12, dependent from claim 1, and claims 16-23 and 25, dependent from claim 14, enjoy the same distinctions.

With respect to the first *prima facie* requirement, the Office Action states that it would have been obvious to combine Seder with Dutta because "the use of encryption shields a recipient's/sender's address

[0015] which is in response to the address of the selected profile in order to decrypt the encrypted data to yield recipient's address [0030]." However, even if this statement were correct, it does not explain how an expert in the art could have modified the Seder reference in such a way as to describe the claimed invention. As explained above in response to the third *prima facie* requirement, even when combined, Seder and Dutta fail to disclose all of the claimed invention limitations. The above-quoted statement from Office Action does not explain how even a person with skill in the art could modify Seder's watermark system to incorporate a user-selected profile to determine a document encryption means and document destination. That is, the assertion does not explain how a person of skill in the art could combine an electronic watermarking system with an address encryption system to yield the claimed profile, or the user selection of a profile to transmit documents. Rather, to meet the first *prima facie* requirement, there must be an explicit teaching that shows an expert how Seder's watermarking system can be replaced or modified in view of Dutta's address encryption. Such a *prima facie* case has not been made, simply because all the Applicant's claim limitations cannot be found in both the Seder and Dutta references.

Alternately, if the Examiner is relying upon the knowledge of a person with skill in the art to supply motivation lacking the Seder and Dutta references, then additional evidence should be provided. Notable, when the source or motivation is not from the prior art references, "the evidence" of motive will likely consist of an explanation or a well-known principle or problem-solving strategy to be applied". *DyStar*, 464 F.3d at 1366, 80 USPQ2d at 1649. The Examiner has not supplied the source for inspiration that an expert could use to modify Seder's electronic

watermarking system into a system that uses a profile with address and encryption fields.

Considered from the perspective of the second *prima facie* requirement, even if an expert were given the Seder and Dutta references as a foundation, no evidence has been provided to show that there is a reasonable expectation of success in the claimed invention.

In summary, the Applicant respectfully submits that a *prima facie* case of obvious has not been supported, and the Applicant requests that the rejection of claims 1-2, 4-9, 11-14, 16-23, and 25-27 be removed.

In Section 5 of the Office Action claims 10 and 23 have been rejected under 35 U.S.C. 103(a) as being unpatentable with respect to Seder and Dutta, in view of Hind et al. ("Hind"; US 6,980,660). The Office Action acknowledges that Seder and Dutta fail to disclose certification authority, but states that it would have been obvious to include the public key encryption of Seder with the certificate authority taught by Hind. This rejection is traversed as follows.

Hind describes a method for encrypting wireless communications. Hind does not disclose the use of profiles, profile address fields, profile encryption fields, or the sending of scanned documents in response to selecting a profile from a directory.

The obviousness rejection appears to be based upon the assumption that the combination of the Seder and Dutta references discloses all the limitations of base claims 1 and 14. However as noted above, the combination of Seder and Dutta fails to disclose a profile with address and encryption fields, the use of such a profile encryption field to encrypt a document, or the use of a profile address field as the document

destination. With respect to the third *prima facie* requirement, even if Hind's certification authority is combined with Seder/Dutta, the combination still does not explicitly disclose every limitation of claims 1 and 14. Claim 10, dependent from claim 1, and claim 23, dependent from claim 14, enjoy the same distinctions.

With respect to the first *prima facie* requirement, the Office Action states that it would have been obvious to combine document encryption as taught by Seder with Hind's certification authority "because Certification Authority verifies the authenticity of the document." However, even if Certification Authority does aid in verifying the authenticity of a document, this statement does not explain how an expert in the art could have modified the Seder reference in such a way as to describe the claimed invention. As explained above in response to the third *prima facie* requirement, even when combined, Seder, Dutta, and Hind fail to disclose all of the claimed invention limitations. The above-quoted statement from Office Action does not explain how even a person with skill in the art could modify Seder's watermark system to incorporate a user-selected profile to determine a document encryption means and document destination. That is, the assertion does not explain how a person of skill in the art could combine an electronic watermarking system with an address encryption system to yield the claimed profile, or the user selection of a profile to transmit documents. Rather, to meet the first *prima facie* requirement, there must be an explicit teaching that shows an expert how Seder's watermarking system can be replaced or modified in view of Hind's Certification Authority. Such a *prima facie* case has not been made, simply because all the Applicant's claim limitations cannot be found in the three references.

Alternately, if the Examiner is relying upon the knowledge of a person with skill in the art to supply motivation lacking the Seder, Dutta, and Hind references, then additional evidence should be provided. The Office Action has not supplied the source for inspiration that an expert could use to modify Seder's electronic watermarking system into a system that uses a profile with address and encryption fields.

Considered from the perspective of the second *prima facie* requirement, even if an expert were given the Seder, Dutta, and Hind references as a foundation, no evidence has been provided to show that there is a reasonable expectation of success in the claimed invention.

In summary, the Applicant respectfully submits that a *prima facie* case of obvious has not been supported, and the Applicant requests that the rejection of claims 10 and 23 be removed.

It is believed that the application is in condition for allowance and reconsideration is earnestly solicited.

Respectfully submitted,

Date: 5/22/2007

Gerald Maliszewski
Registration No. 38,054

Customer Number 55,286
P.O. Box 270829
San Diego, CA 92198-2829
Telephone: (858) 451-9950
Facsimile: (858) 451-9869
gerry@ipatentit.net